A QUANTUM GATE AS A PHYSICAL MODEL OF AN UNIVERSAL ARITHMETICAL ALGORITHM WITHOUT CHURCH'S UNDECIDABILITY AND GÖDEL'S INCOMPLETENESS

Vladan Panković, Milan Predojević
Department of Physics,
Faculty of Natural Sciences and Mathematics,
21000 Novi Sad,Trg Dositeja Obradovića 4.,Serbia and Montenegro,
vladanp@gimnazija-indjija.edu.yu

PACS number : 03.67.Lx

Abstract

In this work we define an universal arithmetical algorithm, by means of the standard quantum mechanical formalism, called universal qm-arithmetical algorithm. By universal qm-arithmetical algorithm any decidable arithmetical formula (operation) can be decided (realized, calculated. Arithmetic defined by universal qm-arithmetical algorithm called qm-arithmetic one-to-one corresponds to decidable part of the usual arithmetic. We prove that in the qm-arithmetic the undecidable arithmetical formulas (operations) cannot exist (cannot be consistently defined). Or, we prove that qm-arithmetic has no undecidable parts. In this way we show that qm-arithmetic, that holds neither Church's undecidability nor Gödel's incompleteness, is decidable and complete. Finally, we suggest that problems of the foundation of the arithmetic, can be solved by qm-arithmetic.

1 Introduction

It is well-known that *usual* arithmetic (and similar theories, i.e. "related systems") according to Church's undecidability theorem [1] and Gödel's incompleteness theorem [2], [3] is *undecidable* and *incomplete*. Or, in the usual arithmetic there are *decidable* formulas (operations), any of

them can be decided (realized, calculated) by universal (arithmetical) algorithm (corresponding, according to Church's thesis [1], to universal Turing's machine). But, also in the usual arithmetic (and *any its extension with similar structure*, called related system) there are *undecidable* formulas (operations) that cannot be decided by universal algorithm. Usual arithmetic considers too that the addition and multiplication (of the natural or whole numbers) are not really the elementary operations since both, by Peano's induction axiom [2], [3], can be reduced in the elementary "the immediate successor of" operation. Finally, usual arithmetic considers implicitly that the universal Turing's machine or any physical model of the universal algorithm works according to classical mechanics.

In this work we shall *firstly* define especial quantum gates, *qm-adder* and *qm-multiplier*. They represent physical models, that works according to quantum mechanics (precisely, *standard quantum mechanical formalism*) [4]-[9], of the algorithms for addition and multiplication. According to standard quantum mechanical formalism (or *mathematical theory of the Hilbert's space of the unit norm vectors*), qm-adder and qm-multiplier represent really the elementary algorithms since neither qm-adder nor qm-multiplier can be reduced in "the immediate successor of" operation. *Secondly*, we shall introduce such *induction rule* according to which an universal arithmetical algorithm, *universal qm-arithmetical algorithm*, can be defined. By qm-universal algorithm *any* decidable arithmetical formula (operation) can be decided. Arithmetic defined by universal qm-arithmetical algorithm, called *qm-arithmetic* , *one-to-one corresponds* to *decidable part of the usual arithmetic*. *Thirdly*, we shall prove that in the qm-arithmetic the undecidable formulas (operations) *cannot exist* (cannot be consistently defined). Or, we shall prove that qm-arithmetic *has no* undecidable parts. In this way we shall show that *qm-arithmetic is decidable and complete* . *Finally*, on the basis of the mentioned proofs, we shall suggest that all problems of the foundation of the arithmetic [1]-[3] can be simply solved by changing of the usual by qm-arithmetic.

2 Quantum adder

We shall define quantum gate for realization of the well-known arithmetical operation, addition, +, (and difference , -) of the whole or natural numbers in an effectively finite time interval. It will be called qm-adder.

Let H be the infinite-dimensional Hilbert's space of the quantum states (vectors) of the unit norm of some quantum system.

It will be pointed out, even if it is well-known, that constant (unit) norm condition represents one of the most important condition of the standard quantum mechanical formalism and corresponding mathematical theory of the Hilbert's space with constant (unit) norm of the states (vectors) [4]-[7]. In other words in given physical formalism or corresponding mathematical theory this condition can be broken neither explicitly nor implicitly. Especially, this condition must be satisfied by unitary symmetric quantum mechanical dynamical evolution on a quantum super-system or sub-system (by "extension" of some sub-systems in a super-system). Also, this condition must be satisfied by measurement on a super-system or sub-system (by "reduction" of some super-system in its sub-systems). For example, states of two sub-systems must have the same unit norm as well as the state of corresponding super-system. All this indicates the following very important consequence. In the quantum mechanics, or in the theory of the Hilbert's space with constant (unit) norm of the vectors, there is none addition (difference) of the vectors norms equivalent to addition (difference) of the whole or natural numbers.

Let $B = ,|-n>,,|-1>,|0>,|1>,,|n>,$ be an especially chosen, called *computational*, complete basis in H.

Let A and B be two quantum systems, first one and second one, whose quantum states belong to B_A and B_B (both equivalent to B) from H_A and H_B (both equivalent to H) respectively.

Let short-lived (which means that here time dependence of corresponding states and operators will not be given explicitly) quantum mechanical dynamical interaction between A and B or quantum mechanical dynamical evolution on the quantum super-system $A+B$ (that holds both A and B representing its sub-systems) be given, in its integral form, by

$$\hat{U}_+|n>|m>=|n>|n+m> \quad for \quad \forall|n>\in B_A, \forall|m>\in B_B \tag{1}$$

Here $\hat{U}_+$ represents the unitary evolution operator determined completely by (1), $|n>$ and $|m>$ on the left hand of the (1) - initial quantum mechanical dynamical states of the A and B, and $|n>$ and $|n+m>$ on the right hand of the (1) - final quantum mechanical dynamical states of the A and B. Of course $\hat{U}_+$ acts over Hilbert's space of the $A+B$, $H_A \otimes H_B$, whose computational basis is $B_A \otimes B_B$, where $\otimes$ represents the tensorial product. More precisely $\hat{U}_+$ one-to-one maps $B_A \otimes B_B$ in the $B_A \otimes B_B$. (In (1) as well as in all further text tensorial product of the quantum states will not be given explicitly.)

Here we shall analyze only states from computational bases. Superposition of the states from the computational bases that unambiguously exists will be not considered. However, it is not hard to see that for $\forall n, m, p, q \in W$ and any real numbers c, d, e, f that satisfy conditions $|c|^2+|d|^2 = 1$ and $|e|^2+|f|^2 = 1$, from the (1) it follows $\hat{U}_+(c|n>+d|p>)(e|m>+f|q>) = ce|n>|n+m> +cf|n>|n+q>+de|p>|p+m>+df|p>|p+q>$. It means that given qm-adder can work by arbitrary superposition of the states from the computational bases, i.e. by "qubits".

Obviously, according to (1), there is one-to-one correspondence between A initial dynamical state $|n>$ and B initial dynamical state $|m>$ on the one hand and first and second addition arguments n and m on the other hand, for $\forall n, m \in W$, where W represents the set of all whole numbers. It means that initial states of the A and B can represent the qm-adder inputs. Also, according to (1), there is one-to-one correspondence between B final dynamical state $|n+m>$ and addition result $n+m$ for $\forall n, m \in W$. It means that B final state can represent the qm-adder output.

So, it is proved that described $A+B$ super-system with quantum mechanical dynamics (1) represents a qm-adder. It can be added that many quantum mechanical super-systems with two sub-systems holds quantum mechanical dynamic equivalent or very similar to (1). For example quantum mechanical dynamics (1) holds interacting measured quantum object and measurement device [4] etc.

It can be observed that different inputs of given qm-adder satisfies practically the same quantum mechanical dynamics (1), i.e. that $\hat{U}_+$ is practically independent of the concrete initial dynamical states of A and B. In other words quantum mechanical dynamics (1) is symmetric in respect to change of given initial dynamical states of the A and B by some other from B_A and B_B. Now we shall show that this symmetry stands conserved by more accurate description of the quantum mechanical dynamical evolution (1) when time dependence of the quantum states and evolution operator is explicit.

For this reason we shall start from differential form of the super-systemic dynamical evolution (1) on $A+B$ generalized in such way that it includes mentioned time dependence

$$(\hat{H}_A \otimes \hat{1} + \hat{1} \otimes \hat{H}_B + \hat{V}_A \otimes \hat{V}_B)|n>|n+m(t)>=$$

$$= (i\hbar\frac{d}{dt} \otimes \hat{1} + \hat{1} \otimes i\hbar\frac{d}{dt})|n > |n + m(t) > for \quad \forall n, m \in W \tag{2}$$

Here $\hat{H}_A$ and $\hat{H}_B$ represents Hamiltonian observable of the isolated A and B, $\hat{1}$ corresponding unit observable, and $\hat{V}_A \otimes \hat{V}_B$ observable of the interaction between A and B, and $|n + m(t) >$ time dependent dynamical state of the B for $\forall n, m \in W$. It will be supposed that $\hat{H}_A$ and $\hat{V}_A$ commute and that B_A represents their eigen basis. Also, it will be supposed that spectrum of the eigen values of $\hat{V}_A$ is nondegenerate. Finally, it will be supposed that initial condition is

$$|n > |n + m(0) >= |n > |m > \tag{3}$$

and that $|n > |n + m(t) >$ tends finally to $|n > |n + m >$ for sufficiently large t for $\forall n, m \in W$. Expression "sufficiently large" would mean infinite large, but, practically there is some effective stopping time $T(n, m)$ determined by (2) and concrete n and m (this determination will not be considered detachedly here), so that

$$< n + m| < n|n > |n + m(t) >=< n + m|n + m(t) >\simeq 1 \quad for \quad t > T(n, m) \tag{4}$$

or

$$< n + m + k| < n|n > |n + m(t) >=< n + m + k|n + m(t) >\simeq 0 \quad for \quad t > T(n, m) \tag{5}$$

for $\forall n, m, k \in W$.

According to introduced suppositions, (2), after partial scalar product by $< n|$, turns formally in the sub-systemic quantum mechanical dynamical evolution on B

$$(\hat{H}_B + v_{An}\hat{V}_B)|n + m(t) >= i\hbar\frac{d}{dt}|n + m(t) > \tag{6}$$

with initial condition corresponding to (3), where v_{An} represents eigen value of the $\hat{V}_A$ in the $|n >$ for $\forall n, m \in W$. Obviously, for any concrete m expression (6) does not represent one dynamical equation but a series of the different dynamical equations any of which is determined by corresponding value of the n, i.e. by initial dynamical state of the A.

But, according to standard quantum mechanical formalism [4]-[10] (that is in full agreement with existing experimental data [11], [12]), it is well-known that super-systemic dynamical evolution (2) on $A + B$ yields a more complete description of the interaction between A and B than sub-systemical dynamical evolution (6) on B, even if both dynamical evolutions yield compatible numerical results. It represents very important fact since it shows that exact dynamical form of the interaction between A and B is exactly independent of the initial dynamical states of the A and B. In other word exact quantum mechanical form of the dynamical interaction between A and B is symmetric in respect to changing of given initial dynamical states of A and B by some other from B_A and B_B. Or, exact quantum dynamics of qm-adder is completely independent of the values of its inputs.

It can be supposed $T(n - k, m) + T(k, m) \geq T(n, m)$ for $\forall n, m, k \in W$ and $|n| > |k|$ and $|n| > |n - k|$. Then, for $t > T(n, m) + T(k, m) \geq T(n + k, m)$, according to (2)-(5) it follows that final dynamical state of B is, practically, $|n + m >$ for $\forall n, m, k \in W$. However, according to standard quantum mechanical formalism [4]-[9], i.e. to linear independence of the states from a (computational) basis, it is satisfied $|n + m >\neq |(n - k) + m > +|k + m >$ for $\forall n, m, k \in W$ and $|n| > |k >$ and $|n| > |n - k|$. It means that quantum mechanical dynamical evolution on $A + B$

(2)-(5) does not admit, even approximately and retrospectively, its representation by a succession of the intermediate outputs on given qm-adder where any of these outputs would be equivalent to addition of the whole numbers.Practically , it implies, that here Peano's induction axiom [2],[3] cannot be satisfied, which will be later (at the end of this section) discussed with more details.

It can be added that in an especial case for $n \geq 0$ and $m \geq 0$ the same qm-adder realizes the addition of two numbers n and m from the set of all natural numbers N.

Further, according to (1), it follows

$$\hat{U}_{+}|n>|-m>=|n>|n-m> \quad for \quad \forall n,m \in W \tag{7}$$

which means that given qm-adder can to realize arithmetical operation inverse to addition, the difference, -, of any two whole number. Also, it means that in an especial case for $n \geq 0$ and $n \geq m$ the same adder can to realize difference between natural numbers n and m.

Finally, following can be observed. According to standard quantum mechanical formalism, i.e. mathematical theory of Hilbert's space of the states (vectors) with unit norm, all states from the computational basis are linearly independent. In this sense none of these states has more complex either simpler structure than any other. In the same sense, all states from computational basis have the same complexity (simplicity). For example, $|n>$, $|m>$ and $|n+m>$ have the same complexity (simplicity) in the B, or $|n>|m>$ and $|n>|n+m>$ have the same complexity (simplicity) in the $B \otimes B$, for $\forall n,m \in W$. (In other words "distance" between arbitrary $|n>$ and $|m>$ from the computational basis, i.e. $|(<m|-<n|)(|n>-|m>)|^{\frac{1}{2}} = 2^{\frac{1}{2}}$ and it is independent of n and m for $\forall n,m \in W$). Finally, according to (1), $\hat{U}_{+}$ acts in the same complex (simple) way at any state from the $B_A \otimes B_B$.

All this points clearly that addition of any two whole (natural) numbers, realized by qm-adder, has the same complexity (simplicity) (in previously defined sense) as the addition of any two other whole (natural) numbers realized by qm-adder. It represents a principal distinction in respect to addition realized by corresponding Turing's machine, i.e. to addition within usual, or, more precisely, Gödel-Turing-Church's, i.e. GTC axiomatic system of the arithmetic, or, simply GTC-arithmetic [1]-[3].

Obviously, both inputs and output of the qm-adder one-to-one correspond to both inputs and output of Turing's machine for addition. It means that here Church's thesis is satisfied. (As it is well-known [1] Church's thesis suggests that *any arithmetical algorithm is equivalent to corresponding especial Turing's machine that belongs to universal Turing's machine.* It can be generalized (which will be discussed later) in the following way which will be used in the further work. *All inputs and output of any algorithm one-to-one correspond to all inputs and output of the corresponding especial Turing's machine that belongs to universal Turing's machine*). But, in GTC-arithmetic, according to Peano's induction axiom, addition represents a complex operation reducible in "the immediate successor of" operation, s,as the simplest, i.e. elementary operation. Namely, since $s(n) = n+1$, it follows $n+m = ss(n)$ (where s is repeated m times), for any two natural numbers n and $m \neq 0$. Equivalently, any natural number n is less complex than natural number $ss(n) = m$ (where s is repeated $m-n$ times), for any natural number $m > n$. (In other words, distance between two natural numbers $m > n$ and n , i.e. $m-n$ depends sharply of the values of these numbers.)

Finally, it is not hard to see that a natural number n in the GTC-arithmetic can correspond to a vector with norm n from the one-dimensional vector space of the vectors without constant norm. Obviously, such one-dimensional vector space of the vectors without constant norm is conceptually

completely opposite to infinite-dimensional Hilbert's space of the vectors with constant (unit) norm.

For this reason, as it is not hard to prove, addition realized by qm-adder cannot be reduced in any simplest operation (here, obviously, is no analogy with "the immediate successor of " operation), or it represents really an elementary operation. All this indicates that qm-adder implies an (axiomatic system of the) arithmetic principally different from GTC-arithmetic, as it will be shown and discussed in the further sections of this work.

3 Quantum multiplier

Now we shall define a quantum gate that realizes other well-known arithmetical operation , multiplication, denoted by or simply by blanc symbol, between any two whole or natural numbers in an effectively finite time interval. It will be called qm-multiplier.

Let A,B be two quantum systems whose quantum states belong to B_A, B_A (all equivalent to B) from the H_A, H_A (all equivalent to H) respectively.

Let short-lived (which means that here time dependence of corresponding states and operators will be not given explicitly) quantum dynamical interaction between A, B or quantum dynamical evolution on the quantum super-system A+B (that holds both A and B representing its subsystems) be given by unitary evolution operator $\hat{U}_\times$. Let $\hat{U}_\times$ satisfies following conditions

$$\hat{U}_\times |n > |m >= |n > |nm > \quad for \quad \forall n, m \in W, n \neq 0 \tag{8}$$

where $|n >$ and $|m >$ on the left hand of the (8) represent initial dynamical states of the A and B, while $|n >$ and $|nm >$ on the right hand of the (8) represent final dynamical states of the A and B for $\forall n, m \in W$. Of course $\hat{U}_\times$ acts over $H_A \otimes H_B$. (For $n = 0$ expression (8) must be especially redefined but we shall not consider this redefinition explicitly. Namely, given redefinition, without any principal problem, needs increase of the technical complexity of the qm-multiplier. If further text, for reason of the simplicity, we shall consider that (8) includes $n = 0$ case too.) Even if $\hat{U}_\times$ is not completely determined by (8) it can be considered that $\hat{U}_\times$ represents an unitary evolution operator that satisfies (8).

Now, we shall prove that $A + B$ represents really a qm-multiplier.

Namely, according to (8) there is one-to-one correspondence between A initial dynamical state $|n >$ and B initial dynamical state $|m >$ and multiplication arguments n and m for n, m ∈ W. In this way initial dynamical states of A and B can represent qm-multiplier inputs. Further, according to (8), there is one-to-one correspondence between B final dynamical state —nm¿ and multiplication result nm for n, m ∈ W. In this way final dynamical state of B can represent qm-multiplier output.

It is obvious that for $\forall n, m, p, q \in W$ and arbitrary real numbers c, d, e, f that satisfy conditions $|c|^2 + |d|^2 = 1$ and $|e|^2 + |f|^2 = 1$ from (8) it follows $\hat{U}_\times(c|n > +d|p >)(e|m > +f|q >) = ce|n > |nm > +cf|n > |q > +de|p > |m > +df|p > |q >$. It means that quantum multiplier can work by arbitrary superposition of the states from computational bases, i.e. by "qubits". But such general situation will not be analyzed in this work.

So, it is proved that described $A+B$ quantum super-system with quantum mechanical dynamics (8) represents a qm-multiplier. It can be added that described qm-multiplier cannot be simply technically realized, i.e. that $A + B$ must be really a very complex quantum super-system that includes many sub-systems. In other words, real qm-multiplier can be only formally, i.e. effectively

presented to be equivalent to $A + B$. But this fact does not represent any principal problem for existence of given $A + B$ qm-multiplier.

On the basis of an analysis, which will not be done explicitly but that is analogous to analysis from the end of the previous section, it can be stated following. Even by more accurate description, when corresponding dynamical states and operators become time dependent, quantum mechanical dynamics of the qm-multiplier is symmetric in respect to changing of the values of qm-multiplier inputs.

Also, multiplication realized by given qm-multiplier is principally different from multiplication realized by corresponding Turing's machine, i.e. multiplication within GTC-arithmetic. Namely, qm-multiplier both inputs and output are one-to-one corresponding to Turing's machine for multiplication both inputs and output which means that Church's thesis is satisfied. But, multiplication in GTC-arithmetic, represents a complex operation reductable in the simpler, addition or "the immediate successor of", i.e. s, operations.(For example, in GTC-arithmetic, multiplication of two natural number n and m can be realized by addition of n natural numbers equivalent to m.) On the other hand, as it is not hard to see, qm-multiplication represents an operation that has the same complexity (simplicity) as qm-addition operation. (For example, $\hat{U}_{\times}|n>|m>=|n>|nm>$ which is different from the $\hat{U}_{+}^{n-1}|m>|m>=|m>|nm>$, for $n-1, m = 1, 2, .$) In this sense qm-multiplication represents really an elementary arithmetical operation.

4 Universal qm-arithmetical gate. Decidable and complete qm-arithmetic

As it is well-known elementary logical operations can be defined by arithmetical operations in following way

$$\neg p = 1 - p \qquad (negation, NO) \tag{9}$$

$$p \wedge q = pq \qquad (conjunction, AND) \tag{10}$$

$$p \vee q = p + q - pq \qquad (disjunction, OR) \tag{11}$$

etc., for $\forall p, q$ that belong to $0, 1$. Here 0 corresponds to logical untruth while 1 corresponds to logical truth. All other composed logical operations according to a logical recursions, i.e. induction rules, can be obtained by an induction by previous elementary logical operations. Roughly speaking usual (propositional) logic represents an especial sub-theory of the arithmetic.

Now we shall determine all possible quantum gates representing physical models of the algorithms, precisely qm-algorithms for realization of corresponding arithmetical (including logical) operations, denoted qm-arithmetical gates, that satisfy following conditions. They work in some effectively finite time intervals and they can be defined recursively, i.e. by inductive combination of the elementary qm-arithmetical gates. Also, it means that given qm-arithmetical gates satisfies Church's thesis.

Ordered series of all such qm-arithmetical gates will be simply called universal qm-arithmetical gate. Also, axiomatic system of the arithmetic based on the universal qm-arithmetical gate will be called qm-arithmetic and its operations - qm-arithmetical operations.

For reason of simplicity in further work we shall not differ explicitly a qm-arithmetical gate and corresponding qm-algorithm for realization of corresponding qm-arithmetical operation. In further simplification we shall not differ explicitly qm-algorithm and corresponding qm-arithmetical

operation if this operation can be realized by given algorithm. In this sense, for arbitrary natural number n, we shall not differ explicitly this number and quantum state $|n>$.

We shall consider that some qm-arithmetical operation is elementary if it cannot be reduced in some other qm-arithmetical operations and if it can be realized (by a qm-arithmetical algorithm) in the completely same way (in the completely same number of the algorithm steps) for any natural numbers that represent its arguments.

Let $M_0(n)$ be unary qm-arithmetical operation (free variable operation) that applied on any natural number n determines given number as the free variable, i.e. that forbids that this number be result of any qm-arithmetical operation. Obviously, given operation does not represent result of any other qm-arithmetical operation. Also, it is satisfied $M_0(n) = n$ for any natural number n which means that given operation is realized in the completely same way for any natural number so that there is no need that its argument value be given explicitly . For this reason given operation can be simply denoted M_0. Thus, M_0 represents an elementary unary qm-arithmetical operation.

Suppose that M_0 represents the unique elementary unary qm-arithmetical operation. (This supposition can be formally-mathematically considered as an axiom.)

Let $M_1(n, k)$ be binary qm-addition qm-arithmetical operation that applied on any natural number n as its first argument and any natural number k as its second argument both representing the free variables yields the result $n+k$. Suppose that qm-addition represents an elementary binary qm-arithmetical operation. Elementarily of the qm-addition follows from the definition of the qm-adder, i.e. from the unitary symmetric quantum mechanical dynamics. (But, this elementarily can be formally-mathematically considered as an axiom.) In accordance with previous discussions and suppositions instead of the $M_1(n, k)$ we can write $M_1(M_0(n), M_0(k))$ or $M_1(M_0, M_0)$ or only M_1.

Further, let $M_2(n, k)$ be binary qm-multiplication, i.e. such qm-arithmetical operation that applied on any natural number n as its first argument and any natural number k as its second argument both representing the free variables yields the result nk. Suppose that qm-multiplication represents an elementary binary qm-operation. Elementarity of the qm-multiplication follows directly from the definition of the qm-multiplier, i.e. from the unitary symmetric quantum mechanical dynamics.(But this elementarity can be formally-mathematically considered as an axiom). In accordance with previous discussions and suppositions instead of $M_2(n, k)$ we can write $M_2(M_0(n), M_0(k))$ or $M_2(M_0, M_0)$ or only M_2.

Suppose that except M_1 and M_2 other elementary binary qm-arithmetical operations do not exist. This supposition follows directly from the characteristics of the unitary symmetry of the quantum mechanical dynamics. (But, this supposition can be formally-mathematically considered as an axiom). Suppose that all other qm-arithmetical operations can be obtained by corresponding rules, i.e. induction starting form the M_0, M_1 and M_2, so that these obtained qm-arithmetical operations are not elementary. Given induction can be realized in the following way.

Firstly, we shall define qm-arithmetical operations

$$M_i(M_j, M_k) \quad for \quad i = 1, 2; j = 0, 1, 2; k = 0, 1, 2; j \neq k. \tag{12}$$

In fact (12) denotes qm-arithmetical operations obtained by application of the qm-arithmetical operation M_i on the qm-arithmetical operation M_j as its first and qm-arithmetical operation M_k as its second argument, under conditions $i = 1, 2; j = 0, 1, 2; k = 0, 1, 2; j \neq k$. Obviously, all given qm-arithmetical operations (12) are well-defined.

Qm-arithmetical operations (12) can be unambiguously enumerated, using (including restriction conditions) lexicographic rules for notation of the variations with repetitions of the elements

M_0,M_1 and M_2 of the third class, in the following way

$$M_3 = M_1(M_0, M_1) \Leftrightarrow n + (m + k) \tag{13}$$

$$M_4 = M_1(M_0, M_2) \Leftrightarrow n + (m \cdot k) \tag{14}$$

$$M_5 = M_1(M_1, M_0) \Leftrightarrow (n + m) + k \tag{15}$$

$$M_6 = M_1(M_1, M_1) \Leftrightarrow (n + m) + (k + l) \tag{16}$$

$$M_7 = M_1(M_1, M_2) \Leftrightarrow (n + m) + (kl) \tag{17}$$

$$M_8 = M_1(M_2, M_0) \Leftrightarrow (n \cdot m) + k \tag{18}$$

$$M_9 = M_1(M_2, M_1) \Leftrightarrow (n \cdot m) + (k + l) \tag{19}$$

$$M_{10} = M_1(M_2, M_2) \Leftrightarrow (n \cdot m) + (kl) \tag{20}$$

$$M_{11} = M_2(M_0, M_1) \Leftrightarrow n(m + k) \tag{21}$$

$$M_{12} = M_2(M_0, M_2) \Leftrightarrow n(m \cdot k) \tag{22}$$

$$M_{13} = M_2(M_1, M_0) \Leftrightarrow (n + m)k \tag{23}$$

$$M_{14} = M_2(M_1, M_1) \Leftrightarrow (n + m)(k + l) \tag{24}$$

$$M_{15} = M_2(M_1, M_2) \Leftrightarrow (n + m)(kl) \tag{25}$$

$$M_{16} = M_2(M_2, M_0) \Leftrightarrow (n \cdot m)k \tag{26}$$

$$M_{17} = M_2(M_2, M_1) \Leftrightarrow (n \cdot m)(k + l) \tag{27}$$

$$M_{18} = M_2(M_2, M_2) \Leftrightarrow (n \cdot m)(kl) \tag{28}$$

Here, on the right-hand sides of $\Leftrightarrow$ explicit forms of corresponding qm-arithmetical operations are given where natural numbers n, m, k, l represent corresponding arguments of M_0, M_1, M_2 and where small brackets denote results of the qm-addition or qm-multiplication.

It is not hard to see that final results of some individual qm-arithmetical operations are mutually equivalent, eg. M_3 (13) and M_5 (15). However, since qm-addition and qm-multiplication are elementarity and mutually different, given individual qm-arithmetical operations, eg. $M_1(M_0, M_1)$ (13) and $M_1(M_1, M_0)$ (15), are different too.

Thus,(13)-(28) define all composite qm-arithmetical operations that can be defined inductively, by one elementary qm-arithmetical operation whose one or both arguments,representing completely free variables,are changed by variables that must have form of some of the elementary qm-arithmetical operations.

Obviously, an ordered enumerable series of all composite qm-arithmetical operations, i.e. universal qm-gate can be obtained by further induction. Concrete technical realization of the universal qm-gate, that unambiguously exists, will not be considered explicitly here.

It is not hard to see too that in any finite step of given induction corresponding composite qm-arithmetical operations, i.e. qm-arithmetical gates work in some effectively finite time intervals. In this sense universal qm-arithmetical operation, i.e. universal qm-gate work in the effectively finite time intervals.

Here, obviously (which will not be proved explicitly), subscript of any composite qm-arithmetical operation is determined unambiguously and it corresponds, practically (i.e. including small corrections), to lexicographic number of the variations of three elements, M_0,M_1 and M_2, of corresponding finite class, with repetitions.

Also, it is not hard to see that all (elementary or composite) qm-arithmetical operations can be divided in the disjunctive classes in the following way.

Zeroth class holds all elementary qm-arithmetical operations M_0, M_1, M_2 whose all, one or two, arguments represent completely free variables.

First class holds all elementary qm-arithmetical operations whose at least one argument represents an elementary qm-arithmetical operation from the zeroth class.

Generally, n-th class holds all elementary qm-arithmetical operations whose at least one argument represents an elementary arithmetical operations from $(n-1)$-th class.

In this way all classes of the qm-arithmetical operations are defined recursively, i.e. inductively.

According to introduced definition of the classes qm-arithmetical operations can be expressed by

$$M_\alpha^k = M_i^0(M_0, M_j^{k-1}) \tag{29}$$

$$M_\beta^k = M_i^0(M_j^{k-1}, M_0) \tag{30}$$

$$M_\gamma^k = M_i^0(M_j^{k-1}, M_m^{k-1}) \tag{31}$$

Here $M_i^0 = M_i$ for $i = 0, 1, 2$ represents an elementary qm-arithmetical operations, i.e. qm-arithmetical operations from the zeroth class ; M_j^{k-1} - qm-arithmetical operations from the $(k-1)$-th class ; and M_α^k,M_β^k,M_γ^k - qm-arithmetical operations from the k-th class

As it is not hard to see (which will not be proved explicitly), subscripts

$$\alpha = \alpha(i, 0, j, k) \tag{32}$$

$$\beta = \beta(i, j, 0, k) \tag{33}$$

$$\gamma = \gamma(i, j, m, k) \tag{34}$$

represent uniquely determined functions of theirs arguments, i.e. subscripts 0, i, j, m, k, more precisely there are one-to-one correspondences between α, β, γ functions and theirs arguments 0, i, j, m, k.

Formally, (29)-(31) can be presented in the following generalized form

$$M_\delta^k = M_i^0(a, b) \quad for \quad i = 1, 2 \tag{35}$$

where either $a = M_0$ and b represent qm-arithmetical operation from the $(k-1)$-th class, either a represents qm-arithmetical operation from the $(k-1)$-th class and $b = M_0$, and where

$$\delta = \delta(i, a, b) \tag{36}$$

represents a formal generalization of (32)-(34).

According to previous discussions and (35), (36) left hand of (35), $M_{\delta(i,a,b)}^k$, represents uniquely determined, $\delta(i, a, b)$-th in the ordered series of the qm-arithmetical operations (from k-th class).

Also, according to previous discussions and (35), (36), right-hand side of (35), $M_i^0(a, b)$, represents uniquely determined zeroth class qm-arithmetical operation, that acting at (a, b) as its argument, yields $M_{\delta(i,a,b)}^k$ as its result.

Finally, it is very important to be pointed out that *according to previous discussions and* (35), (36) *for given* k, *there is no one-to-one correspondence between subscript* i *and* (a, b) *on the one hand , and that subscript* δ *one-to-one corresponds to* (i, a, b) *in* (35), (36) *on the other hand.*

Ordered series of the qm-arithmetical operations (35),(36) for any natural number k represents universal qm-arithmetical operation.

It is not hard to see (which will not be proved explicitly) that final result of any qm-arithmetical operation realized (decided) by universal qm-arithmetical gate one-to-one corresponds to final results of the same qm-arithmetical operations realized (decided) by universal Turing's machine and vice versa. In this way Church's thesis is satisfied.

Now we shall prove that in the qm-arithmetic there are none theorem analogous to Church's undecidability theorem [3] or Gödel's incompleteness theorem [1], [2] existing in the GTC-arithmetic. I.e. we shall prove that qm-arithmetic, in distinction to GTC-arithmetic, is decidable and complete.

As it is well-known [3], Church's undecidability theorem that implies Gödel's incompleteness theorem, can be formulated in the GTC-arithmetic in the following way. In the GTC-arithmetic there is a set S_A of the arithmetical formulas. A formula from the S_A can be denoted by x. Also, in the GTC arithmetic there is an enumerable ordered series of the algorithms simply denoted by k for $k = 1, 2,$ so that $k \in N$. A decidable arithmetical function or operation in the GTC arithmetic $f_k(x)$ represents the result of the action of some arithmetical algorithm k at any formula x. But Church's function $f(x) = f_x(x)+1$ is undecidable. Namely, supposition that $f(x)$ is decidable, i.e. that there is such m for which $f(x) = f_m(x)$, yields, by Gödel-Church's digitalization procedure, i.e. for $x = m$, a contradiction $f_m(m) = f_m(m) + 1$. In this way Church's undecidability theorem, or theorem of the existence of undecidable formulas in GTC-arithmetic is proved.

It is very important that following be pointed out. By definition of a decidable arithmetical function or operation $f_k(x)$, k from the N and x from the S_A represent mutually independent variables. Then, for some fixed k from N, x can hold all possible values from S_A.Without this fact Gödel-Church's diagonalization and Church's undecidability theorem cannot be formulated.

Now suppose that $f_k(x)$ in the GTC-arithmetic can one-to-one correspond to $M_\delta^k = M_i^0(a, b)$ (35),(36) in the qm-arithmetic. Then k from the $f_k(x)$ must correspond to (k, δ) from the M_δ^k and, simultaneously, x from the $f_k(x)$ must correspond to (i, a, b) argument of the δ . But, as it has been discussed, k and x represent mutually independent variables while δ and (i, a, b) are strictly dependent since there is one-to-one correspondence between δ and (i, a, b) . In this way it is shown that previous supposition is incorrect so that there is none unambiguous correspondence between decidable functions or operations in the GTC-arithmetic and qm-arithmetic.

For this reason in the qm-arithmetic a diagonalization procedure analogous to diagonalization procedure in the GTC-arithmetic cannot exist. Moreover, for the same reason, in the qm-arithmetic a theorem analogous to Church's undecidability theorem or Gödel's incompleteness theorem in the GTC-arithmetic cannot exist.

In this way it is proved that given qm-arithmetic is decidable and complete.

5 Discussion and conclusion

As it is well-known Feynman [13], Deutsch [14] and some other scientists suggested that quantum computers, i.e. computers whose working is based on the quantum mechanical dynamics (including its characteristic superposition principle) [15], can be more efficient in the practice than any classical computer (including universal Turing's machine), i.e. computer whose working is based on the classical mechanical dynamics. Really, Shor (Shor's factorization) [16] and Grover (Grover's algorithm for data base search) [17] showed that there are such quantum algorithms realizable by quantum computers that are faster than any classical algorithm realizable by classical computers. Moreover, even if Deutsch [14] proved that classical Church's thesis [1] can be simply (almost "trivially") statistical generalized to be quantum Church's thesis, Grover [18] pointed out : "The

quantum search algorithm is a technique for searching N possibilities in only O(N) steps. Although the algorithm itself is widely known ,not so well known is the series of the steps that first lead to it, these are quite different from any of the generally known forms of the algorithm." In other words Grover's quantum algorithm for data base search is not only faster, but completely different from any Turing's algorithm. All this opens many serious questions not only on the correlations between classical and quantum algorithms but also between (foundation of the) mathematics (arithmetic) and (foundation of the) physics (quantum mechanics). For example, Deutsch [14] states that Church's thesis expresses, in fact, a physical principle, etc..Now we shall discuss some of these questions and we shall suggest some possible answers.

First of all, as it has been presented in the section 2., we use a generalized form of the usual Church's thesis [1]. Namely, we suggest, that generalized Church's thesis needs one-to-one correspondence between all inputs and output of any algorithm and corresponding especial Turing's machine only. Simultaneously we suggest that this thesis does not need necessarily one-to-one correspondence between functional dependence between inputs and output of given algorithm on the one, and, functional dependence between inputs and output of the corresponding especial Turing's machine on the other hand. Thus, generalized Church's thesis can be considered as a consistent general definition of any representation of the decidable part of the arithmetic. Also, in contrast to usual Church's thesis, it admits significantly larger number of the especial representations of the decidable part of arithmetic.

Generalized Church's thesis admits GTC-arithmetic [1]-[3] as an especial case.In this GTC-arithmetic, that includes usual Church's thesis, practically all especial representations of its decidable part are equivalent to mathematical structure of a discrete one-dimensional vector space of the vectors without constant norm . In this space dominant forms of the "motion" are discrete (for natural and whole numbers) translations defined, in fact, by Peano's induction axiom [2],[3]. But such GTC-arithmetic , according to Church's undecidability theorem [1] and Gödel's incompleteness theorem [2],[3], admits existence of the undecidable formulas (operations),i.e. its undecidable parts. In this sense GTC-arithmetic is incomplete.

However, as it has been proved, generalized Church's thesis admits that decidable part of the arithmetic, i.e. qm-arithmetic, be presented in an oposit way, i.e. by mathematical structure of the infinite-dimensional Hilbert's space of the vectors with constant (unit) norm. In this space dominant forms of the "motion" are discrete unitary transformations, i.e. "rotations" (accurate form of the superposition principle!) that one-to-one map computational basis in the same computational basis. (Quite naturally and simply these "motions" can be generalized by such unitary transformations that one-to-one map computational basis in any other basis in given Hilbert's space. In this case superposition principle and existence of the qubits become explicit.) According to well-known characteristics of such "motions" (norm definition in given Hilbert's space) here Peano's induction axiom, Church's undecidability theorem and Gödel's incompleteness theorem cannot be consistently defined. For this reason qm-arithmetic has no undecidable part, or, it is decidable and complete which admits that some principal open problems in the foundation of the arithmetic [1]-[3] can be consistently solved.

Finally, it is very important to be pointed out that mathematical characteristics of the qm-arithmetic are, in fact, completely independent of the physical characteristics of the quantum systems representing qm-arithmetical gates. Or, simply speaking, in distinction to Deutsch opinion [14], Church's thesis does not represent any physical principle. Namely, qm-arithmetic as a mathematical theory is practically completely determined by generalized Church's thesis and mathematical theory of the infinite-dimensional Hilbert's space of the unit norm vectors. But,

since standard quantum mechanical formalism uses the same mathematical theory of the Hilbert's space, qm-arithmetic can be consistently physically modeled by quantum mechanics.

6 References

[1] S.C.Kleene, *Mathematical Logic* (John Wiley and Sons, New York,1967.)

[2] K.Gdel, *On Formally Undecidable Propositions of Principia Mathematica and Related Systems* (Dover, New York, 1992.)

[3] E.Nagel, J.R.Newman, *Gödel's Proof* (New York University Press, New York, 2001.)

[4] J.von Neumann, *Mathematische Grundlagen der Quanten Mechanik* (Springer Verlag, Berlin, 1932.)

[5] P.A.M.Dirac, *Principles of Quantum Mechanics* (Clarendon Press, Oxford, 1958.)

[6] A.Messiah, *Quantum Mechanics* (North-Holand Publ.Co., Amsterdam,1970.)

[7] B.d'Espagnat, *Conceptual Foundations of Quantum Mechanics* (Benjamin, New York, 1976.)

[8] N.Bohr, *Atomic Physics and Human Knowledge* (John Wiley and Sons, New York, 1958.)

[9] N.Bohr, Phys.Rev., **48** , (1935.), 696.

[10] J.S.Bell, Physics, **1**, (1964.), 195.

[11] A.Aspect, P.Grangier, G.Roger, Phys.Rev.Lett., **47**, (1981.), 460.

[12] A.Aspect, J.Dalibard, G.Roger, Phys.Rev.Lett., **49**, (1982.), 1804.

[13] R.Feynman, Found.Phys., **16**, (1986.), 507.

[14] D.Deutsch, Proc.R.Soc.London A, **400** , (1985.), 97.

[15] M.A.Nielsen, I.L.Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000.)

[16] P.Shor, SIAM Journal of Computing, **26**, (1997.), 1484.

[17] L.K.Grover, Phys.Rev.Lett., **79**, (1997.), 325.

[18] L.K.Grover, *From Schrdinger's Equation to the Quantum Search Algorithm*, quant-ph/0109116.